UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,141	12/12/2000	James J. Fitzgibbon	5569-70333	5535

22242 7590 05/29/2008
FITCH EVEN TABIN AND FLANNERY
120 SOUTH LA SALLE STREET
SUITE 1600
CHICAGO, IL 60603-3406

EXAMINER	
HOLLOWAY III, EDWIN C	
ART UNIT	**PAPER NUMBER**
2612	
MAIL DATE	**DELIVERY MODE**
05/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/735,141	FITZGIBBON ET AL.	
	Examiner	Art Unit	
	Edwin C. Holloway, III	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 14-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 14-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

EXAMINER'S RESPONSE

1. In response to applicant's amendment filed 2-28-08, the amendments to the claims have been entered. Claims 1-8 and 14-19 are pending. The examiner has considered the new presentation of claims and applicant's arguments in view of the disclosure and the present state of the prior art. And it is the examiner's position that the claims are unpatentable for the reasons set forth in this Office action:

Claim Rejections - 35 USC § 103

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 1-2, 5, 7-8, 14-16 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu (6041410), Flick (6140939) and Waraksa (5412379).

Regarding claims 1-2, 5, 7-8, 14-16 and 19, Hsu teaches a garage door operating system that includes a fingerprint communicating unit 14 which includes a fingerprint sensor 16, see figures 2 and 3. The communication unit also includes a transmitter 22 that sends a signal to the barrier operator where it is received and authenticated to open the garage door. Hsu does not expressly show the fingerprint comparison occurring at the operator, however in an analogous art, Flick teaches that either having the authentication comparison occur at the

communicating unit or at the barrier operator are both equivalent methods with various pros and cons associated with each. See figures 5 and 6. Hsu does teach that communication from the key to the lock should be encoded or encrypted to prevent cloning by interception. See col. 4 lines 52+. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have the fingerprint authorization occur at the barrier operator as suggested by Flick since it would reduce the processing power necessary in the fingerprint communication unit.

In an analogous art, Waraksa teaches a rolling code used to mix up the id or unlocking code of the portable device which the rolling code changes in accordance with a predetermined algorithm (col. 20 lines 38-47) to prevent cloning and unauthorized access. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have mixed a rolling code with the Hsu-Flick transmission since this would aid in preventing unauthorized access.

4. Claims 3 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Flick and Waraksa as applied above and further in view of Nicholls.

Regarding claims 3 and 17, Hsu-Flick-Waraksa does not expressly disclose use of an electroluminescent fingerprint

sensor. Nicholls discloses an electroluminescent fingerprint sensor called a TactileSense[tm] by Who?Vison[tm] as an improvement over other common fingerprint sensors. It would have been obvious to one skilled in the art at the time of invention to substitute Hsu's optical fingerprint sensor for Nicholls electroluminescent fingerprint sensor since Nicholls discloses an advantage of electroluminescent fingerprint sensors over existing fingerprint sensors, such as the immunity to the 'dry finger problem' that existed in fingerprint sensing technologies at the time of invention (Nicholls, pp 5). Who?Vison[tm] also suggests the integration of such sensors into physical access control devices ("xlvision.com/spinoffs").

5. Claims 4 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Flick and Waraksa as applied above and further in view of Toyoda.

Regarding claims 4 and 18, Hsu-Flick-Waraksa does not teach the use of Charged Coupled Devices (CCDs). Toyoda teaches the use of CCDs to sense fingerprints in the production of identity authentication devices (Fig. 1). It would have been obvious to one skilled in the art at the time of invention to substitute Hsu's optical fingerprint sensor for Toyoda's identity authentication device using a CCD since Toyoda suggests that his device be used to manage entrance and exit of individuals in

restricted areas (Col 1, lines 38- 40) and the use of Toyoda's identification device using CCD would provide an improved individual identification apparatus with a high recognition ability (Col 2, lines 38-42).

6. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Flick and Waraksa as applied above and further in view of Fitzgibbon (5751224).

Hsu-Flick-Waraksa does not expressly show the transmitter comprising a wall controller. In an analogous art, Fitzgibbon '224 shows the use of transmitter 34 that is a wall controller. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have mounted the Hsu-Flick transmitter on the wall of the garage since such would eliminate the need for the user to physically carry around the transmitter.

Response to Amendment

7. The declaration under 37 CFR 1.132 filed 2-28-2008 is insufficient to overcome the rejection of claims 1-8 and 14-19 based upon 35 USC 103 as set forth in the last Office action because:

The inventors opinion is that the prior art discussed in the declaration (Swonger, Plaschko and Scott) establishes that one of ordinary skill in did not understand that wireless

transmission of fingerprints were vulnerable to unauthorized code grabbing. It is noted that Swonger, Plaschko and Scott were not applied by the examiner in the 103 rejections.

The failure of the applicant's cited short passages in the backgrounds of Swonger, Plaschko and Scott to recognize the argued problem cannot be persuasive because the prior art applied by the examiner in the 35 USC 103 rejections does recognize the problem. Hsu recognized that transmitted data related to fingerprint image (CRC derived from fingerprint image) is vulnerable to cloning. Hsu encrypted the data to reduce chances of unauthorized cloning or code grabbing. See col. 4 lines 47-56 and col. 7 lines 44-64 of Hsu. Also, Flick recognized that such a system is vulnerable to unauthorized learning in col. 2 lines 10-13. Waraksa recognized that transmitted codes are vulnerable to theft. Waraksa combined the code with a changing or rolling code in addition to scrambling the result to deter theft similar to Hsu teaching encrypting a the CRC with a changing key in addition to encrypting with a fixed key providing both change over time and scrambling to deter theft.

Applicant's cited passage from Swonger could not have recognized the problem of code grabbing of transmitting fingerprint images because it is not directed to transmitting

fingerprints. But the passage of Swonger does recognize that a card could be lost, loaned or stolen. A transmitter would suffer from similar problems.

Applicant's cited passage form Plaschko recognizes that transmitters have the problem of being lost or stolen. Plaschko reduces this problem by requiring fingerprint input. Other problems are not discussed, nor are they excluded.

Applicant's cited passage form Scott could not have recognized the problem of code grabbing of transmitting fingerprint images because it is not directed to wireless transmission of fingerprints. Contrary to applicant's opinion, the passage of Scott does not disclose that fingerprints are invulnerable, but that fingerprint recognition devices prior to that of Scott were impractical for home or automobile use. The part of the paragraph not cited by applicant goes on to state that this ineffectiveness is due to cost. This teaches that there was a problem with fingerprint systems and other problems may exist. Col. 3 lines 14-16 describes using passwords in addition to the scanned image. This is a recognition that fingerprints alone may not provide sufficient security.

Swonger, Plaschko or Scott lacking recognition of code grabbing is irrelevant because the applied prior art (Hsu, Flick, Waraksa) does recognize problems of cloning, unauthorized

learning and code theft corresponding to code grabbing.

Wuidart (US006164403A) is another patent with remote control transmitter and fingerprint reader that has been cited and not applied in the 103 rejections. Wuidart recognizes in col. 6 lines 13-56 that a code that changed with each transmission (rolling code) is desirable to hinder fraudulent attempts at picking up and recording (code grabbing) the signal.

Response to Arguments

8. Applicant's arguments filed 2-28-2008 have been fully considered but they are not persuasive.

Applicant argues that the declaration of Fitzgibbon establishes that it is true that the prior art did not recognize the problem of code grabbing because fingerprints were thought to be invulnerable. This argument is not persuasive for the reasons stated above under the heading "Response to Argument." Hsu, Flick and Waraksa did recognize vulnerabilities such as cloning, unauthorized learning and code theft corresponding to code grabbing. Further, the art cited but not applied by the examiner in the rejections did recognize vulnerabilities. For example, Scott added a password to increase security in case the transmitter was stolen and Wuidart added a varying or rolling code in case of code recording or grabbing.

Applicant argues that the prior art does not address or

solve the problem of when a bad guys cut off a finger electronically with a code grabber to obtain the code representative of fingerprint data because Hsu and Flick completely rely on use of a signal representing a fingerprint This argument is not persuasive because Hsu and Flick do not completely rely on only use of a signal representing a fingerprint. As stated above, Hsu recognized that transmitted data related to fingerprint image (CRC derived from fingerprint image) is vulnerable to cloning. Hsu encrypted the data to reduce chances of unauthorized cloning or code grabbing. See col. 4 lines 47-56 and col. 7 lines 44-64 of Hsu. Also, Flick recognized that such a system is vulnerable to unauthorized learning in col. 2 lines 10-13.

Applicant argues that the system of the instant application recognizes the problem that if lost to a bad guy, the bad guy can use YOUR rolling code transmitter to get into the house or garage. This argument is not persuasive because Hsu recognizes the problem of a transmitter, card or other device being vulnerable to theft or being stolen (by a bad guy) in col. 1 lines 21-41. Also, the prior art (Swonger, Plaschko and Scott) argued in applicant's declaration recognizes the problem of a lost or stolen card or transmitter.

The argument that Hsu lacked suggestion of combining and

separating codes is not persuasive because the encryption and decryption in Hsu (col. 6 lines 50-65, col. 7 lines 17-34) corresponds to combining and separating codes. The encryption combines the CRC code with key codes and decryption separates the combination.

The argument that Hsu does not suggest transmission of both rolling code and fingerprint data is not persuasive because the CRC is derived from and uniquely identifies the fingerprint image data (col. 5 lines 48-56). Further the CRC is encrypted (combined) with the door public key and the fob (transmitter) private key. A new door key pair is randomly generated with each access (col. 6 lines 42-42, col. 7 lines 13-16) so the keys cannot be determined in advance. This suggests a rolling code.

The argument that Flick lacks suggestion of a rolling code is not persuasive because Hsu provides such a suggestion as indicated in the previous paragraph. The argument Flick, taken alone, lacks suggesting combining a code representative of the fingerprint with an access code and then splitting them is not persuasive because Hsu discloses this as discussed above and Waraksa also teaches combining a transmitter ID and rolling code in cols 10-11 to deter theft and separating the codes in col. 14. The argument that Flick, taken alone, lacks determining whether both fingerprint and rolling code are acceptable is not

persuasive because Waraksa teaches requiring both the ID code and rolling code be acceptable in col. 14 linens 23-49 and Hsu teaches the CRC is a unique ID.

The argument that Waraksa, taken alone, lacks suggesting combining fingerprint code with changing access code and recognizing the fingerprint code as something that needs to be identified is not persuasive because Hsu already suggest this as discussed above. Waraksa discloses combining an ID with a rolling code and scrambling the result. This is suggested by Hsu disclosing encrypting the CRC with a changing public key and then encrypting the result with a private key.

Regarding applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The argument that the art teaches it thought fingerprint data for security is invulnerable is not persuasive because the prior art teaches that fingerprint data (or other data) transmitted in an unsecure manner is vulnerable theft, duplication or cloning.

Applicant argues that the prior art does not suggest a

system that combines the use of signals representative of finger print data to guard against the loss or theft of the transmitter and the use of rolling code to defeat code grabbers. This argument is not persuasive because Hsu suggest fingerprint data to guard against loss or theft of the transmitter (col. 1 line 21 - col. 2 line 57) and the use of rolling code to defeat code grabbers (col. 7 lines 13-16).

Changes to the prior art rejection were necessitated by applicant's amendments.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Setlak (US005828773A) discloses a fingerprint reader (fig. 22) with encrypted output.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action

is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

CONTACT INFORMATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edwin C. Holloway, III whose telephone number is (571) 272-3058. The examiner can normally be reached on M-F from 9:00 to 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman, can be reached on (571) 272-3059.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

5/30/2008 /Edwin C. Holloway, III/
(571) 272-3058 Primary Examiner, Art Unit 2612